Chapter 4 - Operations Security

401 Definition

Operations Security (OPSEC) is defined as "the process of denying adversaries information about friendly capabilities and intentions by identifying the control and protection indicators associated with planning and conducting operations and other activities." The Department's OPSEC program activities are designed to thwart intelligence collection by hostile or adversary interests through the identification of sensitive information, the determination of the collection threat, and the recommendation of countermeasures. OPSEC strengthens the traditional security program by identifying vulnerabilities or weaknesses in the protection collectively afforded by those programs.

402 OPSEC Threat Assessment

A. OPSEC looks at specific missions and projects and analyzes the threats, vulnerabilities, and risks associated with critical information. Department of Commerce managers are encouraged to undertake a five-step process of review to assess OPSEC vulnerabilities. The five-step OPSEC includes:

1. Identification of critical information;

2. Analysis of the threats to the mission under review;

3. Analysis of the vulnerabilities involved in conducting the mission under review;

4. Assessment of the risks involved in the operation of the mission under review; and

5. Application of countermeasures.

B. If any of the factors noted below is missing, there is no need for OPSEC measures to be established. For an OPSEC concern to exist, the following must be present:

1. Critical information to be protected;

2. A threat to the operation or mission, and

3. Vulnerabilities in the operation or mission.

C. OPSEC takes into consideration "risk management." A certain element of risk to an operation is to be expected and handled. Risk management weighs the costs and benefits of countermeasures and strikes a balance between countermeasures and their costs. Risk avoidance may prove to be too costly. In order to manage the risk, OPSEC evaluates all risks prior to determining countermeasures to ensure resources are utilized in the most efficient manner.

403 OPSEC Review Process

A. The following program elements shall be considered when performing an OPSEC review of a program or operational component, or as part of a security compliance review.

1. Define the critical information required to conduct or carry out the mission of the office or program.

2. Define what key elements must be protected from inadvertent, intentional, or premature disclosure.

3. Determine whether a timetable has been established for the disclosure of specific information, and if a timetable is established, and how this timetable is protected.

4. Determine what the threat is, who the adversaries are, and what programs or technologies are vulnerable to the threat.

5. Determine what countermeasures shall be implemented in order to effectively preclude, alleviate, or minimize any known or potential threat.

B. OPSEC reviews shall be conducted for all sensitive activities and facilities whenever:

1. A facility will be constructed that will be used to process or store classified or critical information;

2. New sensitive activities are initiated or significant changes occur to existing programs; or

3. A sensitive program or activity has not been the subject of an OPSEC review, and it is determined that a potential threat or vulnerability to information may be present.

C. For assistance in conducting an OPSEC survey or assessment and in developing an OPSEC Plan for an office or program activity, managers should contact their servicing security officer.

Security specialists are available to assist a program manager in completing a risk analysis and in assessing countermeasures (if any) that need to be in place. Efforts shall be made to strike a balance between cost and effectiveness of the countermeasures.

D. Senior managers in the operating units shall be briefed on the results of any OPSEC surveys or assessments conducted for their activities. The briefing shall include a report of any OPSEC vulnerabilities that have or have not been resolved, the exposed risk, and whether an acceptable risk remains.